REMARKS

Information Disclosure Statement

The applicant submitted an information disclosure statement with the appropriate fee on 06/29/05, a copy of which is included herewith together with a copy of the auto-reply facsimile transmission evincing receipt by the USPTO. The applicant respectfully requests the examiner to consider the IDS and provide an initialed copy of form PTO-1449 in the next office action.

Claim Rejections - 35 USC §103

The examiner rejected claims 1-16 under 35 USC §103(a) as unpatentable over Trieger (US 6,226,750) in view of Stokes. (US 6,473,861) and further in view of Burns et al (US 5,931,947). The applicant respectfully disagrees.

With respect to Claims 1 and 9, the examiner asserts that Trieger discloses a secure disk drive for receiving an encrypted message from a client disk drive, the encrypted message comprising ciphertext data and a device ID identifying the client disk drive. The examiner further asserts that Trieger discloses a secure disk drive that generates a client drive key based on the client drive ID and a secure drive key (state information) for use in authenticating the client drive ID. The applicant respectfully disagrees.

The state information disclosed by Trieger is not a secure drive key. It merely refers to information associated with a particular communication session between a client and a server. The server saves the state information so that the client does not have to resend the state information with each new communication request (see col. 9, lines 20-27). This state information cannot be considered a secure drive key because a client drive key is not generated based on the state information, with an authenticator responsive to the generated client drive key, as recited in the claims.

In Trieger, a server initially authenticates a client by the client sending authentication information, such as a password, to the server (see col. 7, line 65 to col. 8, line 12). If the authentication information is approved, the server generates a first key that identifies the client (device ID), and transmits the key to the client (col. 8, lines 12-15). During a subsequent communication session, the server authenticates the client by validating the key (device ID) sent to the server in a communication request (see col. 8, lines 63-66). As described at col. 9, lines 4-9, Trieger teaches to validate the key by "comparing the value of key 92 with key values stored in a key storage database at the server 52....[or] the key may be self-validating in that the server 52 may be able to immediately recognize the key's information or format." Nowhere does Trieger (or the other relied upon prior art, alone or in combination) disclose or suggest that, when an encrypted message including a client drive ID is received, an authenticator verifies the authenticity of the encrypted message responsive to a client drive key generated based on the client drive ID and a secure drive key.

The examiner asserts that Trieger could be modified in view of Stokes to arrive at the claimed invention. However, Stokes is concerned with encrypting/decrypting data internal to a disk drive (col. 3, line 5 to col. 4, line 12). Nowhere does Stokes disclose or suggest to use secure drive keys together with client drive IDs to facilitate secure communications between disk drives. In particular, nowhere does Stokes disclose or suggest to receive an encrypted message including a client drive ID, or to verify the authenticity of the encrypted message using an authenticator responsive to a client drive key generated based on the client drive ID and a secure drive key. The rejection should therefore be withdrawn.

The examiner asserts that Burns discloses a reply that may also contain an internal drive ID so that devices can authenticate each other. This interpretation of Burns is incorrect. Burns discloses a secure disk drive for authenticating messages received from
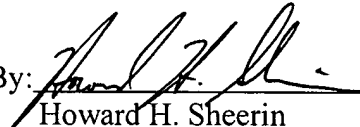
<u>a client user or subscriber and does not disclose devices authenticating each other</u>. (See Abstract, wherein "all encryption is done by the clients, rather than by the devices.") As discussed by the applicant in the specification at page 4, lines 4-6, in Burns, "the keys used by the clients for encrypting data and generating the message authentication codes are generated external to the devices by a system administrator which is susceptible to attack." Since Burns does not disclose or suggest a reply output for outputting reply data and an output for outputting a reply <u>to a client disk drive</u>, Burns cannot be used as the examiner suggests to supplement the disclosure of Trieger.

The rejection of the remaining claims should be withdrawn for at least the reasons set forth above.
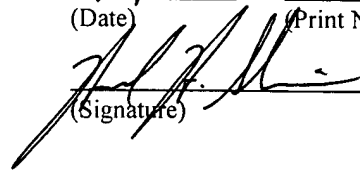
CONCLUSION

In view of the above remarks, the rejections under 35 USC §103 should be withdrawn. The examiner is encouraged to contact the undersigned over the telephone in order to resolve any remaining issues that may prevent the immediate allowance of the present application.

Respectfully submitted,

Date: 1/5/06   By: _____
                    Howard H. Sheerin
                    Reg. No. 37,938
                    Tel. No. (303) 765-1689